What Is Claimed Is:

1. A method for encryption comprising:

a step for storing lock data which includes a public key, an encrypted private key formed by encrypting a private key corresponding to said public key by use of a common key, and a plurality of encrypted common keys generated by encrypting said common key by use of respective public keys of the group/members; and

a step for encrypting encryption target data by use of the public key of said lock data.

2. The method for encryption as claimed in claim 1, wherein said encryption target data is a decrypting key used for decrypting encrypted information.

3. A method for decrypting a cryptogram comprising:

a step for storing lock data which includes a public key, an encrypted private key formed by encrypting a private key corresponding to said public key by use of a common key, and a plurality of encrypted common keys generated by encrypting said common key by use of respective public keys of the group/members;

a step for decrypting one of said encrypted common keys included in said lock data by use of the private key corresponding to said group/member to generate said common key;

a step for decrypting said encrypted private key included in said lock data by use of said decrypted common key to generate said private key;

a step for acquiring encryption target data encrypted by use of said public key; and

a step for decrypting said encrypted encryption target data by use of said decrypted private key.

4. A method for writing a signature comprising:

a step for storing lock data which includes a public key, an encrypted private key formed by encrypting a private key corresponding to said public key by use of a common key, and a plurality of encrypted common keys generated by encrypting said common key by use of respective public keys of the group/members;

a step for decrypting one of said encrypted common keys included in said lock data by use of the private key corresponding to said group/member to generate said common key;

a step for decrypting said encrypted private key included in said lock data by use of said decrypted common key to generate said private key;

a step for storing and acquiring signature target data on which a signature to be verified by use of said public key is to be written; and

a step for writing a signature on said signature target data by use of said decrypted private key.

5. A method for generating lock data comprising:

a step for acquiring a pair of a public key and a private key;

a step for acquiring a common key;

a step for encrypting said private key by use of said

common key to generate an encrypted private key;

a step for encrypting said common key by use of public keys of respective group/members to generate corresponding encrypted common key; and

a step for combining said public keys, said encrypted private key, and said encrypted common keys to generate lock data.

6. A method for generating lock data comprising:

a step for acquiring a pair of a public key and a private key;

a step for acquiring a common key;

a step for modifying said private key by use of a desired function including an inverse function to generate a modified private key;

a step for encrypting said modified private key by use of said common key to generate an encrypted modified private key;

a step for encrypting said common key by use of public keys of respective group/members to generate corresponding encrypted common keys; and

a step for combining said public keys, said encrypted modified private key, and said encrypted common keys to generate lock data.

7. A method for generating lock data comprising:

a step for acquiring a pair of a public key and a private key;

a step for acquiring a common key;

a step for encrypting said private key by use of said common key to generate an encrypted private key;

a step for executing redundant data generating function on respective public keys of group/members to generate redundant data;

a step for encrypting a combination of said common key and said redundant data by use of said respective public keys of group/members to generate corresponding encrypted common keys; and

a step for combining said public keys, said encrypted private key, and said encrypted common keys to generate lock data.

8. The method for generating lock data as claimed in claim 5, wherein said lock data further includes a public key for verifying a signature, an encrypted signature private key which is formed by encrypting a signature private key for writing said signature by use of a public key of a changing right holder, and a signature written by use of said signature private key on desired data included in said lock data.

9. A method for changing lock data comprising:

a step for storing lock data including a first public key, an encrypted private key formed by encrypting a private key corresponding to said first public key by use of a common key, a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective group/members, a second public key for verifying a signature, an encrypted signature private key formed by encrypting a signature private

key for writing said signature by use of a public key of a changing right holder, said first public key, said encrypted private key, said encrypted common key, said second public key, and a signature written by use of said signature private key on said encrypted signature private key;

a step for decrypting said encrypted signature private key included in said lock data by use of said private key of a changing right holder;

a step for changing said lock data; and

a step for writing a signature on the changed lock data by use of said signature private key.

10. The method for changing lock data as claimed in claim 9, wherein said step for changing said lock data includes:

a step for changing said second public key;

a step for changing said signature private key;

a step for changing said encrypted signature private key before changing by use of a new encrypted signature private key newly formed by encrypting a changed signature private key by use of said public key of a changing right holder; and

a step for writing a signature by use of said signature private key after changing.

11. The method for changing lock data as claimed in claim 9, wherein said lock data has a version identifier that indicates the version of said lock data.

12. The method for changing lock data as claimed in claim 9, wherein said lock data has a precedent version dealing identifier, and controls how to deal with the lock data of the

precedent version based on the identifier.

13. The method for changing lock data as claimed in claim 12, wherein said precedent version dealing identifier includes the information that identifies whether the change of said lock data should be applied retroactively or not.

14. A group lock including a public key, an encrypted private key formed by encrypting a private key corresponding to said public key by use of a common key, and a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective group/members.

15. An apparatus for encryption comprising:

a memory part that stores a public key, an encrypted private key formed by encrypting a private key corresponding to said common key by use of a common key, and a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective group/members; and

an encryption part that encrypts encryption target data by use of a public key of said lock data.

16. An apparatus for decrypting an cryptography comprising:

a memory part that stores a public key, an encrypted private key formed by encrypting a private key corresponding to said common key by use of a common key, and a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective group/members;

a generation part that decrypts one of said encrypted common keys included in said lock data by use of said private

key corresponding to a group/member;

a generation part that decrypts said encrypted private key included in said lock data by use of said decrypted common key to generate said private key;

an acquiring part that acquires encryption target data encrypted by use of said public key; and

a decrypting part that decrypts said encrypted encryption target data by used of said decrypted private key.

17. An apparatus for decrypting an cryptography comprising:

a memory part that stores a public key, an encrypted private key formed by encrypting a private key corresponding to said common key by use of a common key, and a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective group/members;

a generation part that decrypts one of said encrypted common keys included in said lock data by use of said private key corresponding to a group/member;

a generation part that decrypts said encrypted private key included in said lock data by use of said decrypted common key to generate said private key;

a memory part that stores and acquires signature target data on which a signature to be verified by use of said public key is to be written; and

a signature part that writes a signature on said signature target data by use of said decrypted private key.

18. An apparatus for generating lock data comprising:

an acquiring part that acquires a pair of a public key and a private key;

an acquiring part that acquires a common key;

a generation part that encrypts said private key by use of said common key to generate an encrypted private key;

a generation part that encrypts said common key by use of public keys of respective group/members to generate an encrypted common key; and

a generation part that combines said public key, said encrypted private key, and said encrypted common key to generate lock data.

19. An apparatus for changing lock data comprising:

a memory part that stores lock data including a first public key, an encrypted private key formed by encrypting a private key corresponding to said first public key by use of a common key, a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective group/members, a second public key for verifying a signature, an encrypted signature private key formed by encrypting a signature private key for writing said signature by use of a public key of a changing right holder, said first public key, said encrypted private key, said encrypted common key, said second public key, and a signature written by use of said signature private key on said encrypted signature private key;

a generation part that decrypts said encrypted signature private key included in said lock data by use of said private key of a changing right holder to generate a signature

private key;

a changing part that changes said lock data; and

a signature part that writes a signature on the changed lock data by use of said signature private key.